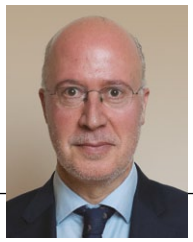
El nuevo Esquema Nacional de Seguridad, un paso más en el fortalecimiento de la ciberseguridad del sector público



La reciente aprobación del nuevo Esquema Nacional de Seguridad ha sentado las bases para afrontar, con un nuevo marco regulatorio firme, la transformación digital del sector público y sus proveedores del sector privado. Y hacerlo con la resiliencia y las medidas de prevención y protección necesarias para afrontar los retos en materia de ciberseguridad que la sociedad actual demanda.

Miguel Ángel Amutio / Pablo López

Una vez aprobado por el Consejo de Ministros, el **nuevo Esquema Nacional de Seguridad (ENS)** se publicó en el Boletín Oficial del Estado el 4 de mayo de 2022, a través del Real Decreto 311/2022, 12 años después de la publicación del primer ENS, como Real Decreto 3/2010, y siete años después de la actualización publicada en 2015.

El primero de ellos, de 2010, que regulaba el ENS en el ámbito de la Administración Electrónica, tenía por objeto determinar la política de seguridad en la utilización de medios electrónicos en todas las entidades de las Administraciones Públicas, estando constituido por los principios básicos y requisitos mínimos para garantizar adecuadamente la seguridad de la información tratada y los servicios prestados.

Desde entonces, **el ENS se ha desarrollado para ofrecer un planteamiento común de principios básicos, requisitos mínimos**, medidas de seguridad, así como mecanismos de **conformidad**, en colaboración con la ENAC, y de **monitorización**, a través del informe INES sobre el estado de la seguridad, junto con las instrucciones técnicas de seguridad, las guías CCN-STIC y las soluciones del CCN-CERT, todo ello adaptado al cometido del **sector público** y de sus proveedores.

La **experiencia acumulada** a lo largo de estos años en la implantación del ENS, la evolución y especialización de los agentes afectados directa o indirectamente, la implantación de la certificación de conformidad con el ENS desde 2016 (que proporciona un amplio conocimiento a partir de las evaluaciones y certificaciones) junto con la constitución del **Consejo de Certificación del ENS** (CoCENS, 2018) han sentado las bases para que este nuevo Esquema Nacional de Seguridad sea una realidad tangible y **adaptada a las necesidades actuales**.

Aumento de exposición

A lo largo de esta década se han intensificado los ciberataques y algunas amenazas, que entonces veíamos como algo incipiente o anecdótico, cuentan ahora con redes organizadas dedicadas a su desarrollo y ataque masivo. Asimismo, la aceleración de la transformación digital, la mayor hiperconectividad y el traslado masivo de todo tipo de actividades al mundo digital (trabajo, educación, ocio, consumo, relaciones sociales) ha **aumentado notablemente la superficie de exposición de los usuarios**.

Por todas estas razones era necesario actualizar el ENS, manteniendo el espíritu de adaptación y actualización constante a la realidad cambiante del ciberespacio. Ya en 2015 se recopilaron numerosos consejos de mejoras posibles desde sectores autorizados, que se incorporaron al conocimiento propio fruto de la experiencia en las auditorías y certificaciones de conformidad más los hallazgos de los equipos del CCN-CERT en la resolución de incidentes de seguridad.

¿Cuáles son los objetivos de la actualización del ENS?

La actualización del ENS ha perseguido, en primer lugar, **alinear el instrumento con el marco normativo** de referencia a la

Figura 1.- Principios, requisitos y medidas de seguridad del nuevo ENS.

fecha para facilitar la seguridad en la administración digital. En segundo lugar, introducir **la capacidad de ajustar los requisitos del ENS a necesidades específicas** de determinados colectivos de entidades, o de determinados ámbitos tecnológicos, dando respuesta a las nuevas demandas. Y, en tercer lugar, **actualizar los principios básicos**, los requisitos mínimos y las medidas de seguridad para facilitar la respuesta a las nuevas tendencias y necesidades de ciberseguridad.

El esfuerzo realizado ha tenido presente el impulso tractor de movilización y transformación, en aras de la ciberseguridad, que supusieron la Estrategia Nacional de Ciberseguridad 2019, el Plan de Digitalización de las Administraciones Públicas 2021-2025, el Acuerdo del Consejo de Ministros de 25 de mayo de 2021 sobre actuaciones urgentes en materia de ciberseguridad y el Plan Nacional de Ciberseguridad, así como la posición de referente internacional, particularmente en la Unión Europea.

Principales novedades

Quienes tengan que aplicar el ENS o se interesen por él verán que se ha realizado la clarificación, precisión, homogeneización, simplificación, o actualización de distintos aspectos del texto, la eliminación de aspectos no necesarios o excesivos, así como la inclusión de nuevos aspectos identificados como necesarios. En particular, encontrarán las cinco grandes novedades que apuntamos a continuación.

En primer lugar, se ha revisado y clarificado el ámbito de aplicación, que alcanza, por un lado, a todo el sector público y, por otro lado, a los sistemas de información de las entidades del sector privado, incluida la obligación de contar con la política de seguridad cuando presten servicios o provean soluciones a las entidades del sector público. Se incluye la referencia a los pliegos de prescripciones administrativas o técnicas, tales como las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS. Además, se extiende su aplicación a los sistemas que manejan o tratan información clasificada.

En segundo lugar, se crea la figura de los **perfiles de cumplimiento específicos** que introducen la capacidad de ajustar los requisitos del ENS a necesidades específicas de ciertos colectivos (Entidades Locales, Universidades, Organismos Pagadores, etc.) o de ámbitos tecnológicos (por ejemplo, servicios en la nube), mediante la definición de un conjunto de medidas de seguridad y para una determinada categoría de seguridad, al objeto de que se pueda alcanzar una adaptación al ENS más eficaz y eficiente sin menoscabo de la protección perseguida y exigible.

En tercer lugar, se ha perfeccionado lo relativo al **tratamiento de los incidentes de seguridad** de forma que se explicita y se clarifica el papel de los principales actores interesados en la cuestión, a la luz del escenario asentado en el Real Decreto-ley 12/2018 y en el Real Decreto 43/2021.

Las entidades públicas notificarán al CCN-CERT los incidentes de seguridad. Las organizaciones del sector privado que presten servicios a las entidades públicas notificarán al INCIBE-CERT, quien lo pondrá inmediatamente en conocimiento del CCN-CERT. El CCN-CERT determinará técnicamente el riesgo de reconexión de sistemas afectados, indicando procedimientos a seguir y salvaguardas a implementar, correspondiéndole la coordinación nacional de la respuesta a incidentes de seguridad informática en materia de seguridad de las redes y sistemas de información del sector público.

Figura 2

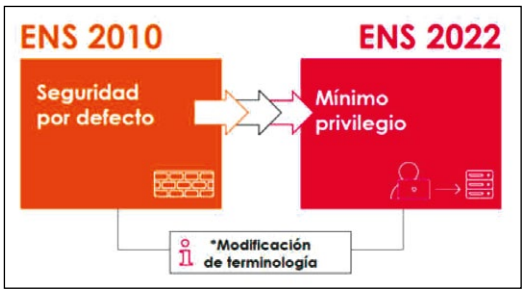


Figura 3

Mientras que la Secretaría General de Administración Digital (SGAD) autorizará la reconexión a los medios y servicios comunes comprendidos bajo su ámbito de responsabilidad, incluidos los compartidos o transversales, si un informe de superficie de exposición del CCN-CERT determinara que el riesgo es asumible.

También se trata el papel de otros actores, como la Oficina de Coordinación de Ciberseguridad del Ministerio del Interior, cuando un operador esencial que haya sido designado como operador crítico sufra un incidente; el ESPDEF-CERT del Mando Conjunto del Ciberespacio (MCCE) cuando un operador con incidencia en la Defensa Nacional sufra un incidente; la Intervención General de la Administración del Estado cuando se trate de un incidente de seguridad que afecte a un medio o servicio común bajo su ámbito de responsabilidad.

En cuarto lugar, se ha realizado una **revisión exhaustiva de los principios básicos, los requisitos mínimos y las medidas de seguridad** que detallaremos a continuación.

En quinto lugar, se ha introducido un **nuevo sistema de codificación de los requisitos de las medidas de seguridad y de sus refuerzos** para facilitar su aplicación y la conformidad.

Las novedades en principios, requisitos y medidas

En cuanto a los principios, se ha incluido como principio básico la 'vigilancia continua' para permitir la detección de actividades o comportamientos anómalos y su oportuna respuesta e impulsar la evaluación permanente del estado de seguridad de los activos, para detectar vulnerabilidades e identificar deficiencias de configuración; y se ha modificado la redacción del principio de 'Prevención, detección, respuesta y conservación', antes denominado 'Prevención, reacción y recuperación'. También se ha clarificado la redacción del principio de 'Diferenciación de responsabilidades' para precisar los aspectos relativos al responsable de seguridad y al responsable del sistema.

Así, los principios básicos que rigen el nuevo ENS y que aparecen enumerados en su artículo 5 son los siguientes: la seguridad integral, la gestión de la seguridad basada en los riesgos, la prevención, detección, respuesta y conservación; la existencia de líneas de defensa; la vigilancia continua y reevaluación periódica y, finalmente, la diferenciación de responsabilidades según los diferentes perfiles dentro de la organización.

En el capítulo de requisitos mínimos se refuerza la importancia de la política de seguridad y el requisito mínimo 'Seguridad por defecto' que pasa a denominarse 'Mínimo privilegio', a la vez que se incluyen diversas mejoras en otros requisitos. Tras estos ajustes la relación de los requisitos mínimos, de obligado cumplimiento, que contempla el nuevo ENS queda como sigue: la organización e implantación del proceso de seguridad; el análisis y la gestión de riesgos; la gestión de personal; la profesionalidad; la autorización y control de los accesos; la protección de las instalaciones; la adquisición de productos de seguridad y

contratación de servicios de seguridad; la norma del mínimo privilegio; la integridad y actualización del sistema; la protección de la información almacenada y en tránsito; la prevención ante otros sistemas de información interconectados; el registro de la actividad y la detección de código dañino; la gestión de los incidentes de seguridad; velar por la continuidad de la actividad y la mejora continua del proceso de seguridad.

En el anexo II de medidas de seguridad se han realizado modificaciones en el marco operacional y en las medidas de protección. Como resultado, algunas medidas han ampliado considerablemente su nivel de exigencia para determinadas categorías (por ejemplo, configuración de seguridad, protección frente a código dañino), y en algunas levemente (por ejemplo, mantenimiento y actualizaciones de seguridad, copias de seguridad). Por el contrario, otras medidas han simplificado su nivel de exigencia (ej. segregación de tareas) y algunas medidas han sido eliminadas o englobadas dentro de otras (ej. Personal alternativo). Además, se han introducido nuevas medidas tales como las relativas a servicios en la nube, interconexión de sistemas, protección de la cadena de suministro que alude a los proveedores o suministradores tecnológicos de las entidades del sector público, vigilancia, otros dispositivos conectados a la red y medios alternativos.

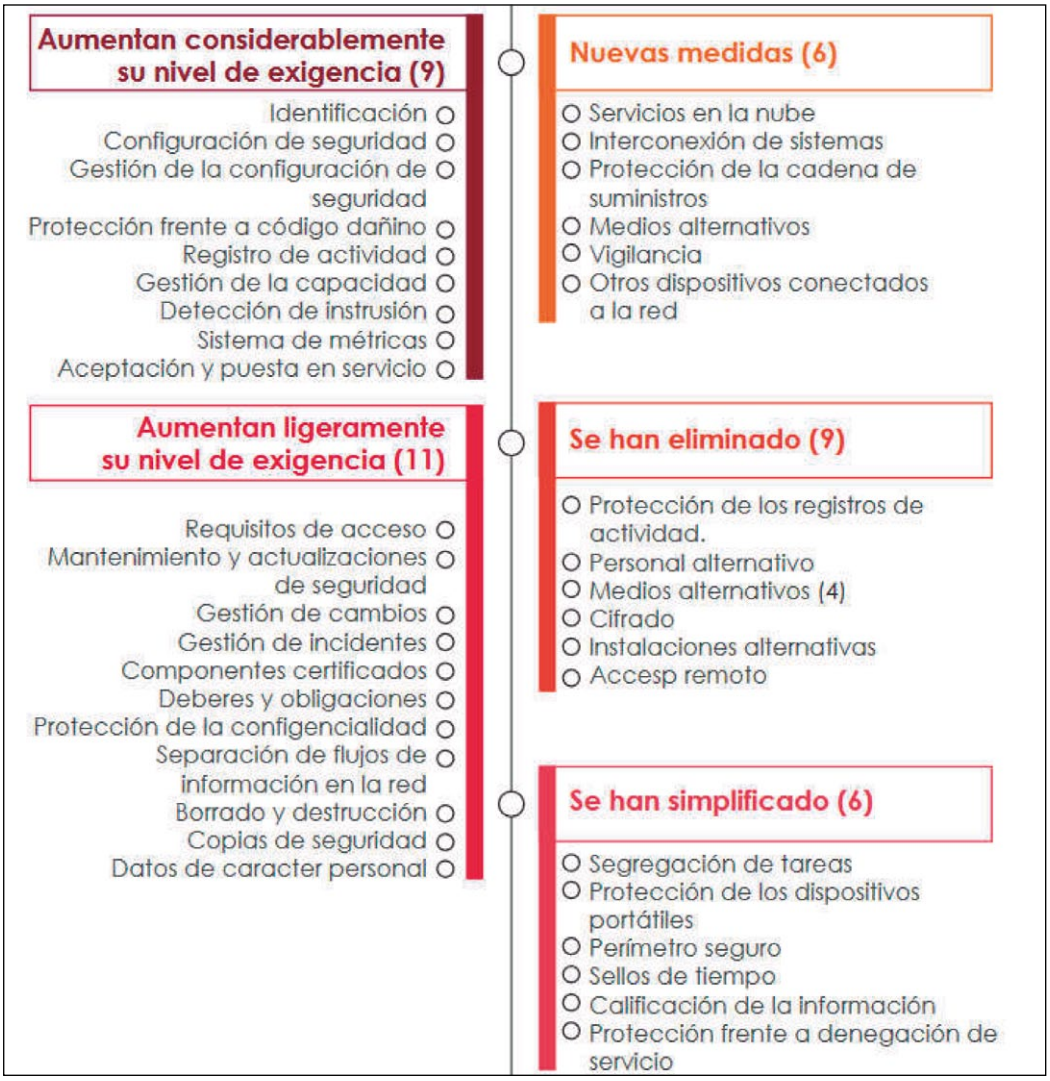


Figura 4.- Resumen de modificaciones a las medidas de seguridad.

La respuesta a incidentes, papel del CCN-CERT

Además de lo expuesto más arriba sobre la respuesta a incidentes de ciberseguridad, el CCN-CERT prestará el servicio de soporte y coordinación del tratamiento de vulnerabilidades y la resolución de los incidentes de seguridad, investigará y divulgará las mejores prácticas sobre seguridad de la información, ofrecerá formación destinada al personal del sector público especialista en el campo de la seguridad informática, así como información sobre vulnerabilidades, alertas y avisos de amenazas a los sistemas de información. En segundo lugar, el CCN desarrollará un programa que ofrezca la información, formación, recomendaciones y herramientas necesarias para que las entidades del sector público puedan desarrollar sus propias capacidades de respuesta a incidentes de seguridad, y en el que será coordinador a nivel público estatal. Este nuevo ENS refuerza el papel mediador y coordinador del Centro Criptológico Nacional, así como de impulsor de formación y herramientas para la adecuación al mismo. Todo ello en aras de conseguir el objetivo último de un ciberespacio más seguro y una administración mejor preparada para los retos que el futuro nos depare en materia de ciberseguridad.

Conclusiones

El nuevo ENS, que se desenvuelve en el **círculo virtuoso** formado por el marco legal, la cooperación y las capacidades de ciberseguridad, constituye un **instrumento esencial para que el sector público y su cadena de suministro sean robustos y confiables, a la vez que, para su protección,** en un escenario en el que los ciberincidentes son crecientes en frecuencia, alcance, sofisticación y severidad del impacto.

El ENS ha supuesto un hito en la ciberseguridad en España y un referente para otros países; una fortaleza que ha posicionado a nuestro país como un referente en la Unión Europea. Bajo el liderazgo de la Secretaría General de Administración Digital en estrecha colaboración con el Centro Criptológico Nacional, junto con sus equipos de colaboradores, el ENS es el resultado de un esfuerzo colectivo de las Administraciones Públicas de España, con la colaboración del sector privado, que vienen contribuyendo activamente a su elaboración, desarrollo, aplicación y evolución. ■

Miguel Ángel Amutio
Director de Planificación y Coordinación de Ciberseguridad
Secretaría General de Administración Digital
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

Pablo López
Jefe del Área de Normativa y Servicios de Ciberseguridad
CENTRO CRIPTOLÓGICO NACIONAL